Scientific Working Group on Digital Evidence

Recommendations for Cell Site Analysis

17-F-001-2.0

Disclaimer and Conditions Regarding Use of SWGDE Documents

SWGDE documents are developed by a consensus process that involves the best efforts of relevant subject matter experts, organizations, and input from other stakeholders to publish suggested best practices, practical guidance, technical positions, and educational information in the discipline of digital and multimedia forensics and related fields. No warranty or other representation as to SWGDE work product is made or intended.

The Scientific Working Group on Digital Evidence requests notification when this document, or any portion thereof, is introduced as a marked exhibit offered for or moved into evidence in any legal proceeding. The notification should include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in the proceeding please notify SWGDE as to the outcome of the matter. Notifications should be sent to secretary@swgde.org.

From time to time, SWGDE documents may be revised, updated, or sunsetted. Readers are advised to verify on the SWGDE website (https://www.swgde.org) they are utilizing the current version of this document. Prior versions of SWGDE documents are archived and available on the SWGDE website.

Redistribution Policy

SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain this SWGDE cover page containing the Disclaimer and Conditions of Use.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or creation date) of the document and also indicate if the document is in a draft status.

Requests for Modification

SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of any suggested modification:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address

d) Telephone number and email address
e) SWGDE Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for suggested modification

Intellectual Property

Unauthorized use of the SWGDE logo or documents without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

Scientific Working Group on Digital Evidence

Recommendations for Cell Site Analysis

Table of Contents

1. Purpose

The purpose of this document is to provide recommendations on the use of Historic Cell Site Location Information contained in Call Detail Records (CDR) when conducting Cell Site Analysis.

2. Scope

This document provides information and recommended guidelines for using Historic Cell Site Location Information contained within CDRs to conduct Cell Site Analysis. The intended audience for this document are practitioners who have training, knowledge, and experience in using these investigative techniques, which may include investigators, analysts, and attorneys. This document is not intended to be a training manual or to replace standard organizational procedures. This document is not all-inclusive and does not account for every possible scenario related to Cell Site Analysis, and it should not be confused with mobile device forensics. Refer to SWGDE Best Practices for Mobile Phone Forensics for details of mobile device forensics best practices, linked here. Historic Cell Site Location Information may be obtained through other means, including law enforcement surveillance activities such as pen register/trap and trace of devices with cell site information, mobile device forensics, and location data which may exist in cloud-based or remote locations. While obtaining the location information through other means can be invaluable, the focus of this document is limited to Historic Cell Site Location Information contained within the CDRs, as maintained by the cellular service providers relative to Cell Site Analysis.

3. Definitions

The following definitions are provided to assist with interpreting this document. For further details, readers may refer to more technical resources defining these terms, such as Third Generation Partnership Project (3GPP) and European Telecommunications Standards Institute (ETSI) (http://webapp.etsi.org/Teddi/).

4G, LTE – Fourth generation Long Term Evolution (LTE) is a standard for wireless communication of high-speed data for mobile phones and devices.

5G – 5th Generation cellular network technology. Offering higher transmission speeds than 4G with lower latency.

Actual Beamwidth (ABW) – The coverage that is not always reported by a cellular service provider for a cell site sector's coverage but is the true beamwidth that the cell site sector actually covers. This is also known as total coverage area.

Addressing and Routing Data – Data that represents the transactional data of an electronic communications event. This data includes such items of data as the phone numbers dialed, durations of phone calls, phone numbers involved in text messages, Internet Protocol (IP) addresses involved in data transactions, etc. This data does not include the contents of any electronic communications.

Antenna – An electrical device which converts electric power into radio waves, and vice versa. It is usually connected with a radio transmitter or radio receiver and can be mounted on various structures including poles, masts, towers, etc.

Automated Cell Site Analysis Mapping Program – Software that automates the analysis and plotting of locations contained within the CDRs.

Azimuth – The direction an antenna is pointed in degrees where zero is north. With a cell site sector, the azimuth represents the center point of the sector's coverage. Azimuth is also known as orientation.

Base Transceiver Station (BTS) – A piece of equipment that facilitates wireless communication between user equipment and a network. User equipment includes devices such as mobile devices or computers with wireless Internet connectivity. The network can be any of the wireless communication technologies like GSM, CDMA, wireless local loop, Wi-Fi, or other wide area network (WAN) technology.

Beamwidth – The radio frequency arc of coverage of an antenna, measured in degrees. With a cell site sector, half of the beamwidth is represented counterclockwise, and the other half of the beamwidth is represented clockwise from the azimuth. Beamwidth in cell site analysis typically represents the Horizontal Beamwidth (HBW) of coverage of a sector. Vertical Beamwidth (VBW) can represent an antenna's uptilt or downtilt.

Call Detail Record (CDR) – Records maintained by the service provider capturing information typically needed to accurately bill a subscriber or, in the case of a prepaid service plan, debit the balance. This information typically includes the date, time, duration, source identifier, destination identifier, or the amount of data transmitted or received.

Cell Site – A cell site is a physical location that contains the equipment needed to receive and transmit radio signals for cellular voice and data transmission and may consist of equipment from one or more cellular telephone companies. Cell sites are designed to provide radio frequency coverage over defined geographic areas.

Cell Site Analysis – The analysis of historical records provided by the cellular companies, or other geographic data, in order to place a particular cellular device within an approximate, and possibly even fairly-specific, geographic area during a specified date and time.

Cell Site List – The list of all cellular system antennas with sector information that is retained by a cell provider. Cell site lists typically contain the latitude and longitude of cell sites as well as specific sector information including the azimuths and beamwidths of sectors.

Cellular Service Provider – A cellular service provider is a wireless communications service provider that owns or controls all the elements necessary to sell and deliver services to an end user including radio spectrum allocation, wireless network infrastructure (antennas and switches), backhaul infrastructure, provisioning computer systems and repair organizations. Examples of cellular network providers are AT&T, T-Mobile, and Verizon Wireless. This can also be known as cellular network operator, mobile network operator, and wireless carrier.

Code Division Multiple Access (CDMA) – A spread spectrum technology for cellular networks based on the Interim Standard-95 (IS-95) from the Telecommunications Industry Association (TIA). Is a form of multiplexing a radio signal that allows multiple signals to occupy a single transmission channel.

Distributed Antenna System (DAS) – A network of relatively small antennas within a geographic area or structure.

DRAS – Dialing, Routing, Addressing, and Signaling information of electronic communication events including phone calls, text messages, data transactions (i.e., IP), etc.

Geolocate – Real-time, precision location requests from the device in a surveillance capacity. Geolocates are commonly referred to as "pings" and will normally reflect a latitude and longitude along with a certainty factor. Geolocates may be produced through various means, and several major cell phone providers can provide law enforcement geolocates on a target device. A geolocate may require some form of legal process.

Global Positioning System (GPS) – A system for determining position via latitude and longitude by comparing radio signals from several satellites.

Global System for Mobile Communications (GSM) – A set of standards for second generation cellular networks currently maintained by the 3rd Generation Partnership Project (3GPP).

Heat Map – A geographical representation of RF coverage where the individual signal strengths are represented as colors.

Historic Cell Site Location Information – The historical communications data contained within a Call Detail Record.

Internet Protocol (IP) – The principal communications protocol used to move data across the Internet, and most Intranets, via packets of data.

Latitude and Longitude – A coordinate system that enables every location on the Earth to be specified by a set of numbers.

Mobile Virtual Network Operator (MVNO) – A wireless communications services provider that does not own the wireless network infrastructure over which the MVNO provides services to its customers. An MVNO enters into a business agreement with a cellular network operator to obtain bulk access to network services at wholesale rates, then sets retail prices independently.

Neighboring Cell Sites – Cell sites that are in close proximity to the target cell site. Neighboring Cell Sites can affect the outer boundaries of a target cell site's coverage area.

Omni-Directional Cell Site (AKA Omnipole) – A cell site that contains only one sector with 360° of coverage.

Optimal Beamwidth (OBW) – The coverage that is reported by a cellular provider that reflects the best, or optimal, coverage area of a particular sector. Optimal beamwidth does not typically reflect the absolute coverage area of a particular sector.

Pen Register (related Trap and Trace) – A law enforcement surveillance technique that monitors and records, in real time or near real time, the outgoing destination identifiers (i.e., dialed phone numbers) of a target's phone calls, text messages, data transactions, or other electronic communications. Pursuant to appropriate legal authority, pen registers can also provide the cell site and sector, and location data related to the device for these communication events.

Radio Frequency (RF) – Any of the electromagnetic wave frequencies that lie in the range extending from around 3 kHz to 300 GHz, which include those frequencies used for communications or radar signals. RF usually refers to electrical rather than mechanical oscillations.

Radio Frequency Survey – A survey of radio frequency signals using sophisticated equipment and antennas. This provides a detailed map of the radio frequency coverage for a specific geographic area.

Radio Frequency Propagation Map – A geographical representation of RF coverage, not necessarily including signal strengths, which displays the approximate boundaries of a cell site.

Sector – The section of a cell site that covers a specific geographic area.

Sector Line – The line that is drawn to establish the approximate outer clockwise and counterclockwise boundary of a sector, measuring in degrees from the azimuth. This is also known as the edge of the sector and is determined by the azimuth and beamwidth. This line is for illustration purposes only and does not reflect the exact coverage area of the sector.

Specialized Historic Location Data – A measurement of the time it takes for a signal to be transmitted from the Base Transceiver Station (BTS) at the cell site to a remote cellular device and back to the BTS. Ranging data may also be reported as Range to Tower (RTT), Round Trip Delay (RTD), Real Time Tool (RTT), Per Call Measurement Data (PCMD), Reveal Data, Timing Advance, etc. Specialized historic location data provides distance from cell site antenna estimates along an arc within sectors.

Survey – see Radio Frequency Survey.

Tower – A cellular telephone site where an antenna and electronic communications equipment are placed on a radio tower mast to create a cell site(s) in a cellular network.

Trap and Trace (related Pen Register) – A law enforcement surveillance technique that monitors and records, in real time or near real time, the incoming origination identifiers contacting a target. This can include incoming telephone numbers involved in phone calls, text messages, data transactions, or other electronic communications. Pursuant to appropriate legal authority, a trap and trace device can also provide the cell site and sector, and location data related to the device for these communication events.

4. Considerations

Cell Site Analysis only demonstrates the specific cell site and sector (if applicable) used by a particular cellular device at a specific date and time. CDRs do not conclusively indicate who was using a device but can be used to establish patterns of use. Furthermore, cell site and sector

information in CDRs do not allow for the identification of an exact location of a device at a specific date and time (e.g., a specific intersection, address, etc.).

An advanced method of Cell Site Analysis not detailed in this document includes the utilization of RF survey equipment to establish detailed cellular signal propagation estimates. These more detailed RF estimates may be displayed on RF propagation maps (i.e., frequency-coverage heat maps). RF analysis requires specific experience, knowledge, training and equipment, and is not covered in this document.

Historic Cell Site Location Information may be obtained through other means, including law enforcement surveillance activities such as, pen register and trap and trace of devices with cell site information, mobile device forensics, and location data which may exist in cloud-based or remote locations.

5. Future Considerations

This document was prepared with the resources available at the time of publication. As with all technology, Cell Site Analysis is a constantly evolving discipline, with frequent implementation of new features and innovations. As time progresses, the data available from cellular providers will change, as will the formats in which the available data is provided. Additional empirical studies on how cell phone signal things work could also shape future best practices and standards.

6. Call or Communications Detail Records Data Preservation, Procurement, Documentation, and Archiving

6.1 Introduction

Cellular service providers maintain records through the normal course of business or as required by law, which contain certain historical information, to include CDRs with Historic Cell Site Location Information. This information can be obtained through an appropriate legal process. Additionally, data may also be available from other sources, including data from non-cellular providers which are considered official business records, from the forensic extraction of mobile devices, from law enforcement surveillance activities (e.g., pen registers), and potentially even cloud-based or remote locations.

It is beyond the scope of this document to discuss, in detail, various legal avenues an analyst might pursue to preserve or obtain CDRs with Historic Cell Site Location Information. Those seeking Historic Cell Site Location Information should consult with legal counsel for specific guidance in a particular investigation within their jurisdiction. Practitioners are encouraged to become familiar with the particulars of each of these possible legal channels. Federal, state, and local laws might also provide guidance. Practitioners should always be mindful to comply with their own organization's policies and procedures. In order to preserve or obtain CDRs with Historic Cell Site Location Information, practitioners may make use of one or more of the following legal instruments, which may be applicable in certain jurisdictions.

6.1.1 Preservation Requests

Title 18 U.S. Code § 2703(f) provides law enforcement officials with the ability to order the preservation of records and other evidence held by an electronic communications provider. Preservation requests allow law enforcement to order providers to preserve data. In doing so, data that may otherwise be perishable (e.g., deleted by the provider) is preserved for a specified period of time prior to obtaining the appropriate legal authority to secure the release of the preserved data.

6.1.2 Customer Consent

Electronic communications service providers may be able to release customer-related data to law enforcement officials with customer consent. Additional information relating to consent can be found in Title 18 U. S. Code § 2702(c)(2).

6.1.3 Lawful Emergencies and Exigent Requests (e.g., kidnappings, hostages, etc.):

Federal and some state laws allow for the immediate and voluntary release of Cell Site Analysis data by providers in certain specific emergency situations. Consult Title 18 U.S. Code § 2702(b)(8). Providers may require submission of their "Exigent" form prior to providing records. Also, your jurisdiction may require you to follow your Exigent request with legal process.

6.1.4 Subpoenas, Search Warrants, and Court Orders

The most common method of obtaining Historic Cell Site Location Information from CDR data through a criminal investigation is with a search warrant or, where permitted, other appropriate court orders.

In civil matters, civil court rules allow for the use of a subpoena or court order.

Legal issues change rapidly and are subject to interpretation, therefore always consult with your appropriate local legal counsel or prosecutor regarding all legal matters before acting.

6.2 Service of Legal Demands

In order to obtain Historic Cell Site Location Information data from cellular providers, personnel requesting the data will typically need to serve legal demands to electronic communications providers. While service in person may be possible, legal demands are typically served electronically (e.g., email, website service), or via fax. It is important that both original and copies of legal demands be preserved and that the service of legal process be appropriately documented.

6.3 Obtaining Cell Site Lists and Reference Sheets and Court Admission Issues

In addition to the specific Cell Site Analysis data itself, it is also important to obtain any applicable cell site lists from the time in question. This information will aid in indicating where cell site antennas are located and how they are configured in the involved geographic areas. Despite the specific latitude and longitude references to the antennas used by a target device in a CDR, it is necessary to have the neighboring cell site locations and information. This aids to

conduct Cell Site Analysis more thoroughly. It is also important to compare the latitude and longitude coordinates listed in the CDRs to ensure they are consistent with the cell site list.

Other useful data includes any available reference sheets, instruction sheets, or legends that may be available to assist in properly interpreting the provided data. For example, time zones may be reported in various ways, and it is imperative that the appropriate time zone is determined for the location of the device. It is also important to obtain a cell site list for the appropriate time period (e.g., not using a 2016 list when analyzing 2011 records).

Finally, if use of the records in court is anticipated, it is important to prepare to meet any applicable rules of evidence requirements. To ensure admissibility of these business records in court, it is typically sufficient to obtain a business records affidavit for the CDRs, subscriber information, any Specialized Historic Location Data, cell site list(s), and any applicable instruction pages or legend documentation. Practitioners should exercise caution, as records may be purged by the time these affidavits are requested. It also may be important to use a local jurisdiction's business records affidavit (e.g., from the state where the prosecution is occurring) rather than a business records affidavit from the state where the records are held or produced, if applicable.

6.4 Potentially Available Location Data Other than Historical CDR Cell Sites

Additional location information may be available in the form of engineering and switch data, mobile device forensic data, and pen register/trap and trace devices. Practitioners should recognize that this data may not be held long and will require additional expertise to properly obtain, interpret, analyze, and present.

6.5 Documentation

Practitioners should document the process and procedures used to conduct Cell Site Analysis. It is important to document where, how, when, and by whom the data was obtained. Additionally, documentation should include specifically what data was obtained and how the data was archived. Finally, those conducting Cell Site Analysis should also maintain current documentation, such as a detailed curriculum vitae (CV) that thoroughly details their qualifications to conduct Cell Site Analysis. The CV should include formal education, training, case experience, and relevant experience in the field of Cell Site Analysis.

7. Data Interpretation

Historic Cell Site Location Information used in Cell Site Analysis is typically obtained from historical CDRs sourced from the cell service providers. Historic Cell Site Location Information may also be obtained in real-time from legally-authorized surveillance, namely, pen registers and trap and trace of devices. It may also be possible to obtain reliable location data from cellular devices utilizing mobile device forensics. Refer to "SWGDE Best Practices for Mobile Phone Forensics for details of mobile device forensics best practices," linked here. Those conducting Cell Site Analysis should be familiar with the type of records produced by the various service providers and the intricacies, nuances, and limitations associated with each provider.

7.1 Formats of Different Cellular Providers

Cellular providers produce records in various formats. While the CDRs from various cellular providers may look very different, they generally contain the same basic information, including the date and time of the event, the originating and terminating phone number, duration, and cell site and sector information at the initiation of the event. It is important to properly interpret the information and recognize the differences in key terms from the various cellular providers. A CDR reference document, also known as a "carrier key," should be requested from each cellular provider when legal process is served.

7.2 Cellular Service Provider versus Mobile Virtual Network Operators

A cellular service provider is a wireless communications service provider that owns or controls all the elements necessary to sell and deliver services to an end user, including radio spectrum allocation, wireless network infrastructure (antennas and switches), backhaul infrastructure, provisioning computer systems, and repair services. Examples of cellular service providers include but are not limited to AT&T, T-Mobile, and Verizon Wireless.

A MVNO is a wireless communications service provider that does not own the wireless network infrastructure over which the MVNO provides services to its customers. An MVNO enters into a business agreement with a cellular network service provider to obtain bulk access to network services at wholesale rates. The MVNO then resells network access and sets retail prices independently. Examples of a MVNO are Straight Talk and TracFone.

It is important to note that in order to obtain records, data, or surveillance access on an MVNO cell phone, contact must also be made with the cellular network providing service to the device, in addition to the MVNO.

7.3 Differences in Time Zone Reporting

Service providers report CDRs in various time zones. For example, times could be reported in the time zone where the device is located, where the switch is located, a centralized location for the provider, or, commonly in Universal Coordinated Time (UTC).

Caution must be taken when analyzing CDRs in preparation for converting listed times to local times, if required. Additional caution should be exercised regarding Daylight Savings Time (DST), when applicable, as not all jurisdictions observe DST. In some circumstances, a switch may encompass multiple time zones, which could impact time adjustments for accurate analysis. A single CDR could also contain a mix of time zones based on different regions of the United States, as well as change to or from DST.

7.4 Pen Registers/Traps and Trace Devices

Pen registers/traps and traces are real-time, or near real-time, surveillance actions conducted by law enforcement. Pen registers and traps and traces provide real-time cell site and sector information for the target device, along with Dialing, Routing, Addressing, and Signaling data such as date, time, and sender and receiver identifiers. This data does not include the content of any communications.

As a result, Cell Site Analysis may be conducted with pen register or trap and trace data in addition to historical CDRs. However, practitioners should be aware that more data may be available in CDRs than is available in pen register and trap and trace data.

8. Processing the Data for Casework or Lead Purposes—Preliminary Reporting

Practitioners frequently conduct preliminary analysis and mapping to aid investigative efforts. Those conducting Cell Site Analysis for these purposes should exercise caution when placing too much confidence in Cell Site Analysis findings without additional verification. Practitioners will often conduct Cell Site Analysis under short time constraints. In doing so, various methods may be used to report preliminary results such as verbal reporting, quick hand-drawn maps, automated cell site analysis mapping program, etc. For example, images may be captured via screen capture utilities, sent in emails, or attached to other documents. While effective, those conducting Cell Site Analysis should always strive to accurately report the data and reduce confusion related to findings, especially with lay personnel. It is recommended that any preliminary reporting reflect a disclaimer representing that the product is in draft form and has not been fully verified.

9. Processing the Data for Court and Legal Proceedings—Final Reporting

When processing Cell Site Analysis data for court or legal proceedings, additional steps should be taken to ensure that the analysis was properly conducted and verified (including manual validation). Additionally, working with maps must be done with care so that presentations preserve aspect ratios (are not distorted) and include a scale that is unaltered by resizing maps. Those conducting Cell Site Analysis should follow their organization's quality standards, which may include peer-review, to ensure validity of the work product and that the analysis is accurate and repeatable. Finally, those presenting Cell Site Analysis in a legal setting should coordinate with attorneys before any court presentation of Cell Site Analysis.

10. Mapping the Data

10.1 Omni-Directional Cell Site vs. Sectorized Cell Site

Omni-directional cell sites transmit their RF signals in all directions from a single antenna. The single antenna provides 360-degree coverage from the site. Orientation cannot be determined from an omni-directional cell site. A sectorized cell site utilizes directional antennas oriented to provide coverage to a specific geographic area. The most common type of sectorized cell sites utilize three (3) antennas to complete 360-degree coverage around the tower. See Figure 1 below for an example of Omni-Directional vs. Sectorized Cell Site.

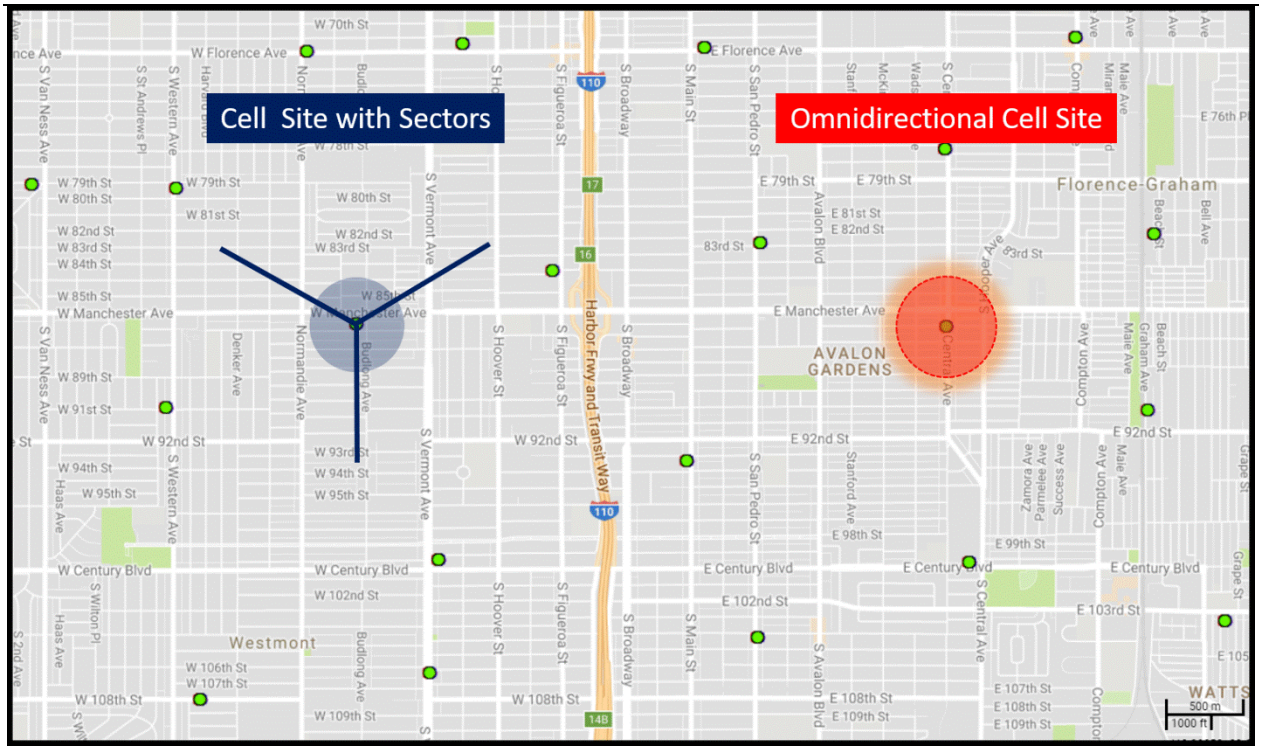

Figure 1. Omni-Directional vs. Sectorized Cell Site Example

10.2 Sectors

Cell Sectors are utilized by service providers to increase coverage and capacity within a specific geographic area. Sectors are oriented in a specific direction to provide coverage and limit interference from other sectors. The predominant configuration used by cellular providers are three (3) separate sectors, each providing approximately 120-degrees of coverage, and therefore providing a 360-degree coverage around the cell tower. There are other configurations that may exist; for more information, consult the cellular service provider cell site list. Coverage is not always uniform across all sectors and can vary from cell site to cell site.

For an example of a sector coverage area, see figure 2 below.

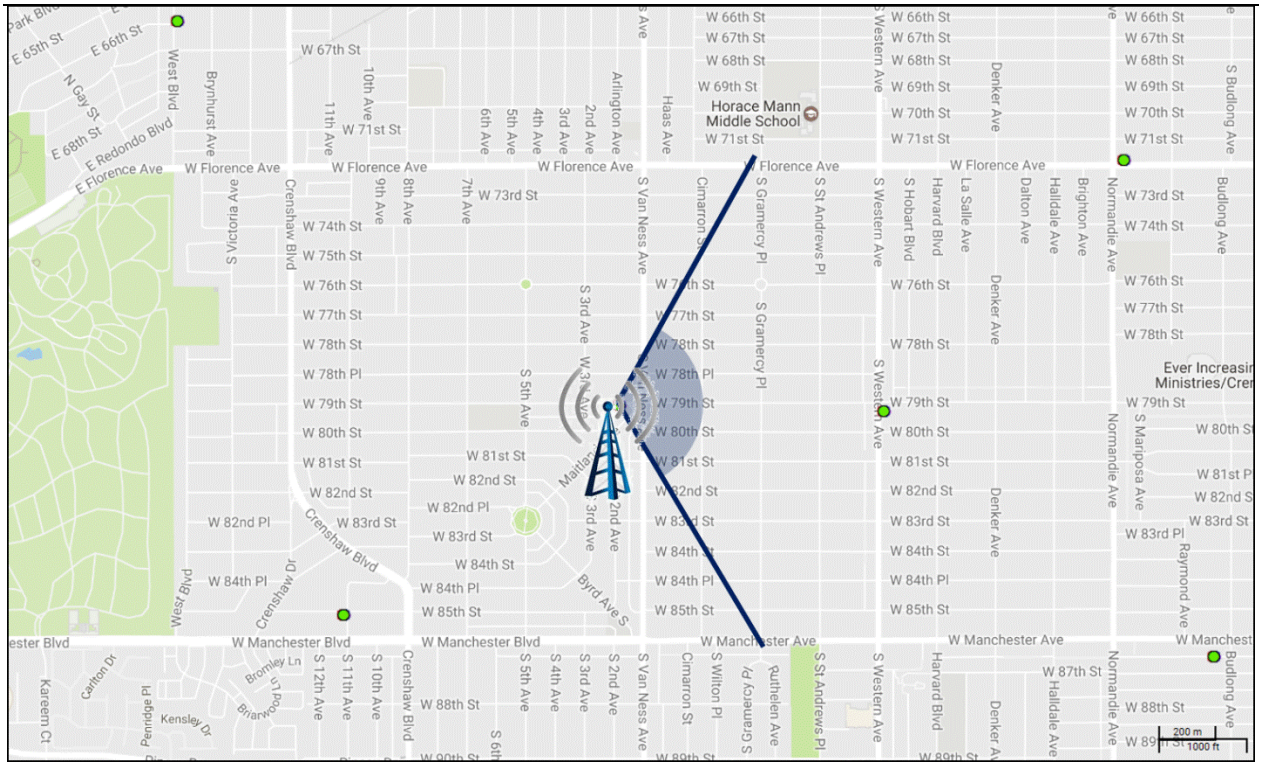

Figure 2. Example of a Sector

10.3 Azimuth and Orientation

The azimuth, also known as an orientation, is the direction representing the center of a sector's beamwidth. The azimuth bisects the sector's beamwidth and is represented in degrees. See Figure 3.

10.4 Horizontal Beamwidth

This is the measurement of the angle of the sector, represented in degrees. Half of the beamwidth is on each side of the azimuth (counterclockwise and clockwise from the azimuth). Half Beamwidth is -3dB (half power) from the azimuth of the antenna. This should not be considered the absolute edge of the sector coverage. See Figure 3.

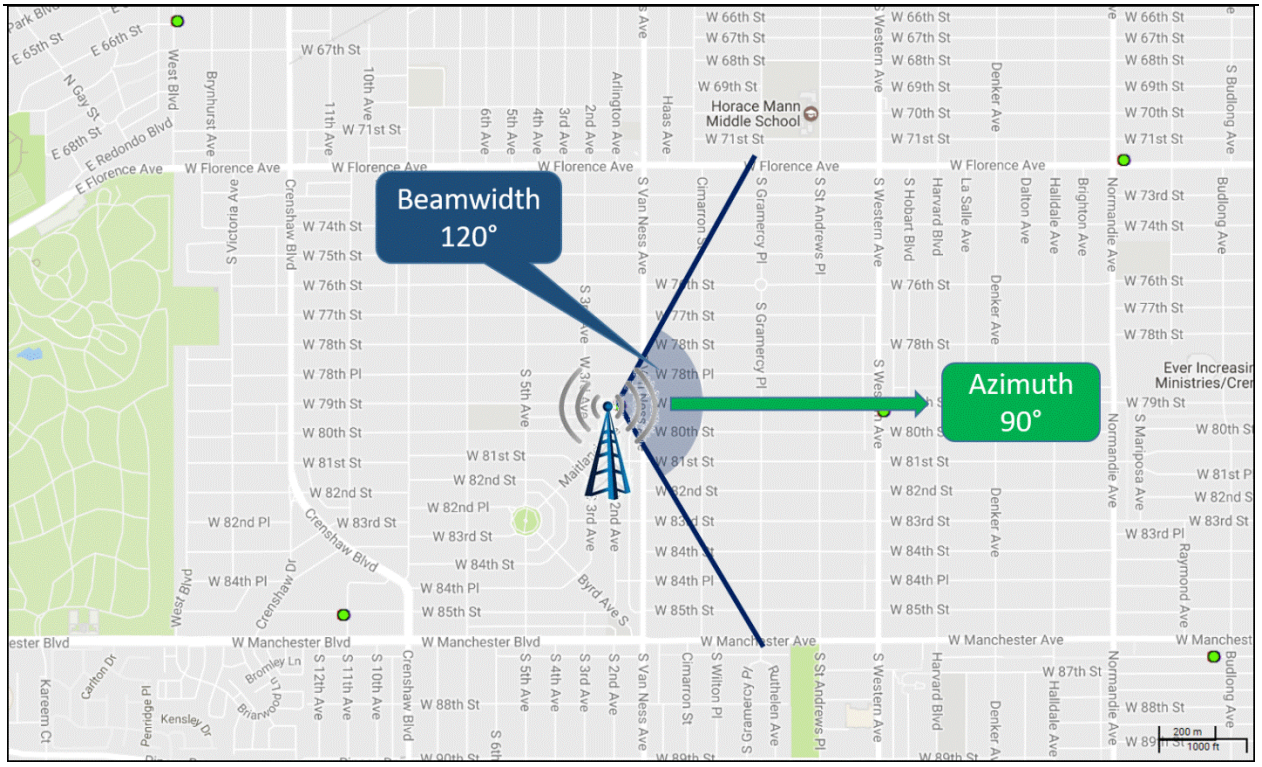

Figure 3. Example of Azimuth and Beamwidth Measurements

10.5 Optimal Beamwidth versus Actual Beamwidth

Optimal Beamwidth, which is fewer degrees of coverage than the actual beamwidth, is the horizontal beamwidth that is often reported by the service provider and consists of the strongest area of coverage within the center of the sector's beamwidth of coverage. Actual beamwidth is the total geographic area of the sector in which there would be coverage. Cell site sectors' actual beamwidths cover approximately 120-degrees. Beamwidth may vary and should be verified with service providers as needed. Caution should be utilized when working with optimal beamwidths and actual beamwidths to not underestimate a sector's actual coverage.

10.6 Specialized Historic Location Data

Cellular service providers often maintain Specialized Historic Location Data for engineering and network optimization purposes through the normal course of business. The retention for these types of records can be relatively short, and requests to preserve the records should be made as soon as possible after an incident. Specialized Historic Location Data provides an approximate distance of the mobile device from the cell site. Specialized Historic Location Data are derived from the measurement of the time required for the signal to travel from the cell site to the handset and then back to the cell site. In some cases, confidence levels related to these measurements are provided. Specialized Historic Location Data is non-technology specific and can be found in GSM, CDMA, LTE, and 5G networks. In some cases, service providers also

provide an estimate of the approximate location of the device via latitude and longitude with varying confidence levels. The coordinates provided in these types of records are generated from a proprietary algorithm and are not intended to provide an exact location of a device. As a result, it is recommended that Specialized Historic Location Data be mapped at the listed approximate distance from the cell site within the provided sector.

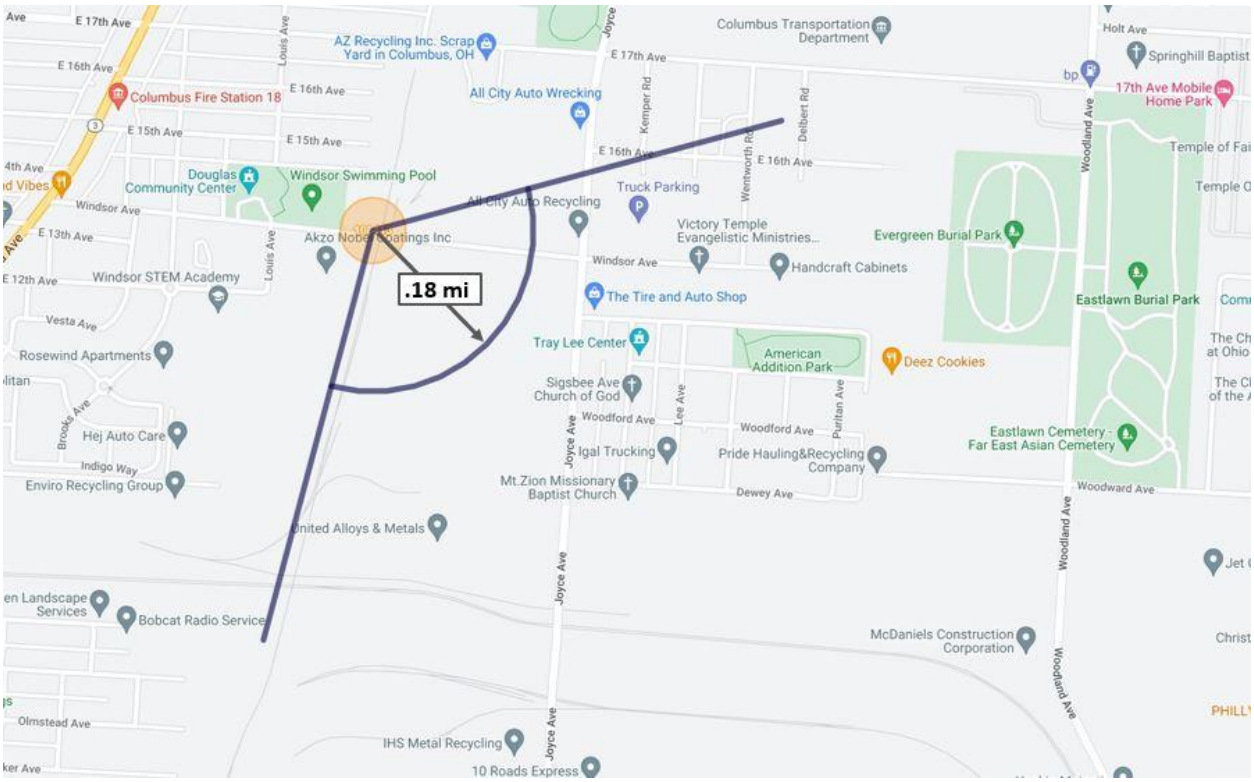

Figure 4. Example of Specialized Historic Location Data as shown with cell site, sector, and approximate distance from cell site.

10.7 Precision Geolocation Information

Geolocates are real-time, precision location requests from the cellular network to the device, requesting the device's location. Geolocates are commonly referred to as "pings" and will normally report a latitude and longitude along with a certainty factor or margin of error from that point. It is extremely important to map the certainty factor, or radius, that is reflected in the geolocate data. Simply mapping the latitude and longitude commonly will not provide a valid result on its own. Further, geolocate data is not kept in the normal course of business and is typically not obtainable from the service providers as official business records at a later date, and, if obtained, should be archived.

A Geolocate example is provided below in Figure 5.

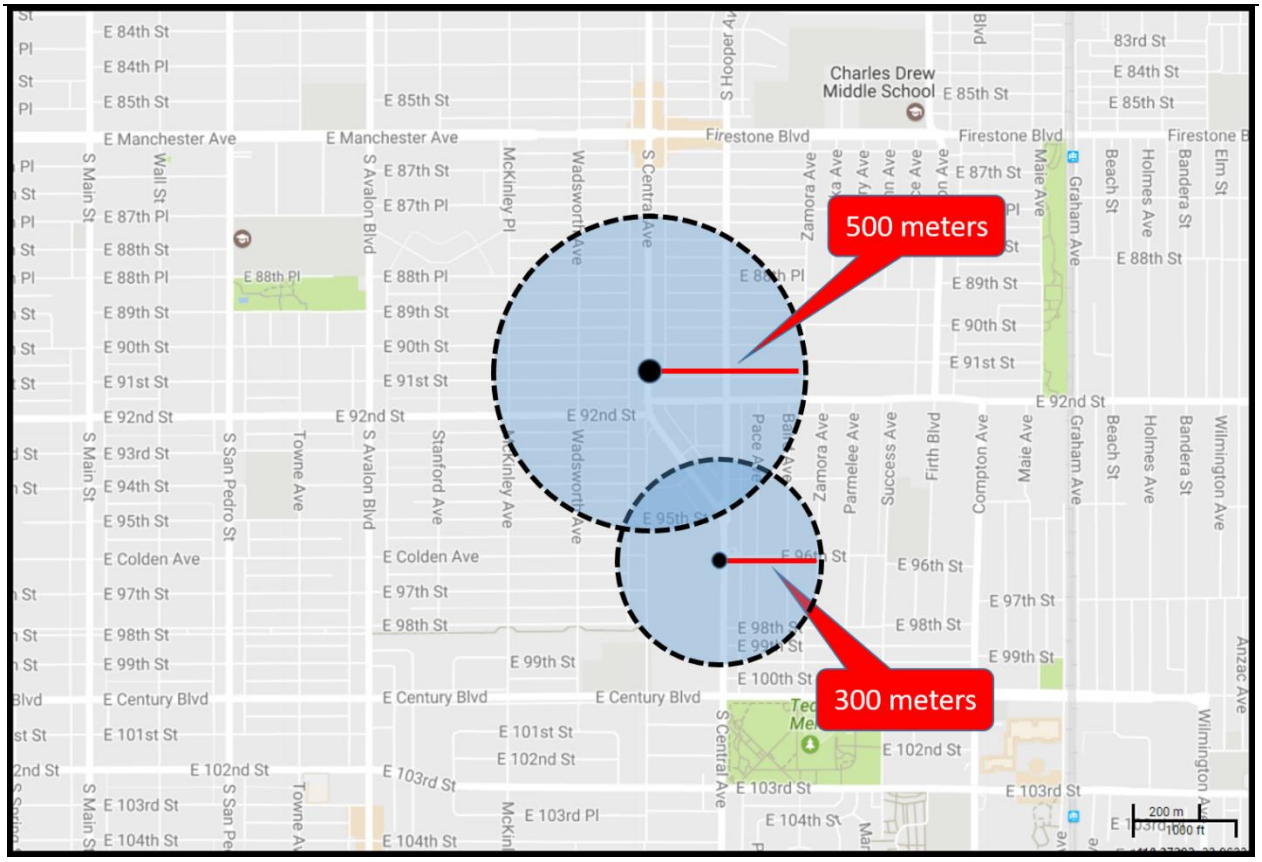

Figure 5. Example of Geolocates

10.8 Data Sessions

Data session records are available from the cellular service providers for internet enabled devices. The records can include the date and time, bytes sent from the device to the cell site, bytes from the cell site to the device, IP information, and may include location information. When using this data for location purposes, the records should be verified and validated because the time stamps and data associated with these records can vary amongst cellular service providers.

11. Verification

Those conducting Cell Site Analysis should be able to verify results by manual mapping of sampled data or using alternate automated cell site analysis mapping programs with different underlying methodology. When using automated programs to plot and report the location data for formal legal proceedings, those conducting the analysis should be able to explain how the software or tool works and be able to validate the accuracy of the final results by mapping manually. Completed analysis should undergo technical review to ensure an accurate result. Analytic approaches should be well documented and reproducible.

12. Presenting the Data in Legal Proceedings

Cell Site Analysis practitioners should properly represent map data by providing legends and distance scales that present proportionally-accurate maps. In addition, practitioners should consult and coordinate with their appropriate legal counsel.

As a general rule, courts require the witness presenting Historic Cell Site Location Information to be admitted as an expert witness. The witness needs to have relevant knowledge, training, and experience interpreting CDRs. Those conducting Cell Site Analysis should be prepared to present a thorough CV detailing this relevant knowledge, training, and experience. Legal considerations such as Daubert and Frye standards, or any other applicable expert witness legal requirements, may apply.

13. Additional Resources

[1] United Kingdom Accreditation Service (UKAS), "ISO/IEC 17025 Accreditation for Forensic Cell Site Analysis – An Overview – Pilot Update July 2016," May 5, 2016. Available: https://www.ukas.com/accreditation/about/developing-new-programmes/development-programmes/forensic-cell-site-analysis/.

[2] CSIR Built Environment, "Analysis and Mapping of Cellular Telephone Usage. Contract Report: Sea Point CAS," Pretoria, South Africa, June 14, 2009.

[3] P. Schmitz, A. Cooper, A. Davidson and K. Roussow, "Breaking Alibis through Cell Phone Mapping," Crime Mapping Case Studies: Successes in the Field, Volume 2, pp. 65-72, 2000. Available: https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=183202.

[4] “Cell Phone Analysis,” ESRI ArcGIS for Local Government, 22 April 2017. [Online]. Available: http://solutions.arcgis.com/local-government/help/cell-phone-analysis/.

[5] A. Edens, Cell Phone Investigations: Search Warrants, Cell Sites and Evidence Recovery, Police Publishing, ISBN: 978-1-63180-006-1, 2014.

[6] K. Metcalf, Cell Phones in Criminal Investigations: Basic Preparation, Analysis, and Mapping of Cellular Data, Amazon Digital Services LLC, 2016.

[7] "Cell Site Analysis and Mapping," Forensic Magazine, 23 January 2013. [Online]. Available: http://www.forensicmag.com/product-release/2013/01/cell-site-analysis-and mapping-0. [Accessed 22 April 2017].

[8] G. Smith, "Checking Masts – Cell Site Analysis (CSA)," Forensic Focus,15 July 2011. [Online]. Available: https://www.forensicfocus.com/articles/checking-masts-cell-site-analysis-csa/. [Accessed 21 June 2022].

[9] "Appendix: digital forensics: cell site analysis. Part of: Forensic science providers: codes of practice and conduct," Forensic Science Regulator of United Kingdom, Ref: FSR-C-135, 9 June 2016. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/918946/135_FSR-C-135_Cell_Site_Analysis_Issue_2.pdf.

[10] P. Schmitz, C. Eloff, R. Talmakkies, C. Linnen and R. Lourens, "Forensic mapping in South Africa: four examples," Cartography and Geographic Information Science, vol. 40, no. 3, pp. 238-247, May 2013. [Online]. Available:

http://dx.doi.org/10.1080/15230406.2013.800273.

[11] J. Hoy, Forensic Radio Survey Techniques for Cell Site Analysis, West Sussex: Wiley, February 23, 2015.

[12] R. Ayers, S. Brothers and W. Jansen, "Guidelines on Mobile Device Forensics," NIST Special Publication 800-101, pp. Section 6.3, pages 52 through 54, May 2014. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf.

[13] M. Tart, I. Brodie, N. Gleed and J. Matthews, "Historic cell site analysis – Overview of principles and survey methodologies," Digital Investigation, vol. 8, no. 3-4, pp. 185-193, February 2012.

[14] B. Siuru, "How Can Cell Phone Records Help to Solve Crimes?," Police and Security News, pp. 44-46, September/October 2014. [Online]. Available:

https://policeandsecuritynews.com/imgs/archives/2014/digital/SeptOct2014.pdf.

[15] U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, “Investigative Uses of Technology: Devices, Tools, and Techniques," NIJ Special Report, pp. 11, 13, 17, 31, 33, and 102, October 2007. [Online]. Available:

https://www.ncjrs.gov/pdffiles1/nij/213030.pdf.

[16] P. Schmitz and A. Cooper, "Mapping Crime Scenes and Cellular Telephone Usage," South Africa)., 2000. [Online]. Available: http://hdl.handle.net/10204/2788.

[17] P. Schmitz, A. Cooper, T. De Jong and D. Rossmo, "Mapping Criminal Activity Space,” Journal of Intelligence and Analysis, vol. 22, no. 3, pp. 67-94, December 2015.

[18] C. Miller, " The Other Side of Mobile Forensics,” Officer.Com, 1 July 2008. [Online]. Available: http://www.officer.com/article/10248785/the-other-side-of-mobile-forensics.

[19] T. O’Connor, "Provider Side Cell Phone Forensics," Small Scale Digital Device Forensics Journal, vol. 3, no. 1, June 2009. [Online]. Available:

http://ctfdatapro.com/pdf/celltower.pdf.

[20] H. B. Dixon Jr., "Scientific Fact or Junk Science? Tracking a Cell Phone without GPS,” The Judges' Journal, vol. 53, no. 1, 2014. [Online]. Available:

https://www.americanbar.org/publications/judges_journal/2014/winter/scientific_fact_or_junk_science_tracking_a_cell_phone_without_gps.html.

[21] I. Ajala, "Spatial Analysis of GSM Subscriber Call Data Records," Directions Magazine. 8 March 2006. [Online]. Available: http://www.directionsmag.com/entry/spatial-analysis-of gsm-subscriber-call-data-records/123196.

[22] A. Cooper and P. Schmitz, "Tactical Crime Mapping in South Africa," Networks and Communication Studies, NETCOM, vol. 17, no. 3-4, pp. 269-279, 2003. [Online]. Available:

https://www.researchgate.net/profile/Antony_Cooper2/publication/228410584_Tactical_Crime_Mapping_in_South_Africa/links/00b49527b96fdd8e6f000000.pdf?origin=publication_detail.

[23] P. Schmitz, S. Riley and J. Dryden, "The Use of Mapping Time and Space as a Forensic Tool in a Murder Case in South Africa," in Proceedings of the 24th International Cartographic Conference, Santiago de Chile, Chile, November 19, 2009. [Online]. Available: http://icaci.org/files/documents/ICC_proceedings/ICC2009/html/refer/20_5.pdf.

[24] T. O'Malley, "Using Historical Cell Site Analysis Evidence in Criminal Trials," United States Attorneys' Bulletin, vol. 59, no. 6, pp. 16-34, November 2011.

[25] V. M. Jovanovic and B. T. Cummings, "Analysis of Mobile Phone Geolocation Methods Used in US Courts," in IEEE Access, vol. 10, pp. 28037-28052, 2022, doi: 10.1109/ACCESS.2022.3156892. [Online]. Available: https://ieeexplore.ieee.org/document/9729192

[26] N. Chemello, "Correlating CDR with other data sources," 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF), 2016, pp. 1-5, doi: 10.1109/ICCCF.2016.7740425. Correlating CDR with other data sources | IEEE Conference Publication | IEEE Xplore

14. History

Revision	Issue Date	History
1.0 DRAFT	9/15/2016	Initial draft created and SWGDE voted to release as a Draft for Public Comment.
1.0 DRAFT	10/8/2016	Formatting and technical edit performed for release as a Draft for Public Comment.
1.0 DRAFT	1/12/2017	Full rewrite performed on the initial draft; title changed to remove "Forensic" before "Cell Site Analysis." SWGDE voted to re-release as a Draft for Public Comment.
1.0 DRAFT	2/21/2017	Formatting and technical edit performed for re-release as a Draft for Public Comment.
1.0 DRAFT	6/22/2017	Additional revisions were made to all sections for finalization. SWGDE voted to re-release as a Draft for Public Comment.
1.0 DRAFT	7/11/2017	Formatting and technical edit performed for re-release as a Draft for Public Comment.
1.0	8/24/2017	SWGDE voted to publish as an Approved document (Version 1.0).
1.0	9/25/2017	Formatted and published as Approved Version 1.0.
2.0	9/21/2022	Formatting and technical edit performed for re-release as a Draft for Public Comment.